lmat2440

2023

Number theory

UCLouvain

5.00 credits	30.0 h + 15.0 h	Q1

Teacher(s)	Caprace Pierre-Emmanuel ;Caprace Pierre-Emmanuel (compensates Pereira Olivier) ;Pereira Olivier ;
Language :	French > English-friendly
Place of the course	Louvain-la-Neuve
Prerequisites	It is recommended that the student master the fundamental notions of linear algebra as developed in e.g. LMAT1131 or LEPL1101.
Main themes	Introduction to various aspects of number theory and its methods, in particular with a view to its application to mathematical cryptography.
Learning outcomes	**At the end of this learning unit, the student is able to :**

	1	Contribution of the course to the learning outcomes of the Master's programme in mathematics. **At the end of this activity, the student will have progressed in his/her ability to :** - Know and understand a basic foundation of mathematics. In particular, he/she will have developed the ability to : -- Select and use the fundamental methods and tools of calculation. -- Recognize the fundamental concepts of important current mathematical theories. -- Establish the main links between these theories. - Demonstrate abstraction, reasoning and critical thinking skills. In particular, he/she will have developed the ability to : -- Identify the unifying aspects of different situations and experiences. -- Reason within the framework of the axiomatic method. -- construct and write a demonstration in an autonomous, clear and rigorous way. - To analyze a mathematical problem and propose adequate tools to study it in an autonomous way. Learning outcomes specific to the course. **At the end of this activity, the student will be able to :** - solve equations in rings of modular integers; - determine existence conditions for solutions of certain Diophantine equations; - apply results of mathematical analysis to the study of prime numbers; - apply results of modular arithmetic to the construction of algorithms used in cryptography. **How students' achievements are assessed :** The assessment is based on a written examination. The knowledge and understanding of fundamental notions, examples and results, the ability to construct a coherent reasoning, the mastery of demonstration techniques introduced during the course are tested.

Evaluation methods	The assessment is based on a written exam, testing the knowledge and understanding of the theoretical notions, the examples and fundamental results, the ability to develop a consistent reasoning, and the mastery of the proof techniques introduced during the lectures. One or several mini-projects may be proposed during the quadrimester, and contribute to a maximum of 25% of the final grade for the course. This contribution is taken into account only if it is beneficial to the student.
Teaching methods	The course is taught by means of theoretical lectures and exercise sessions. During the sessions, the students are invited to make suggestions and formulate their ideas to advance the course on the basis of their preliminary knowledge.
Content	This activity consists in illustrating various aspects of number theory, including some that can be applied to cryptography. The following themes will be tackled. - Modular arithmetic: Chinese remainder theorem, quadratic reciprocity. - Rational quadratic forms: p-adic numbers and local-global principle. - Analytic methods: zeta function and Dirichlet's theorem. - Projective cubics: arithmetic properties of elliptic curves. - Algorithmic number theory: primality tests, factorization. - Construction of objects relevant to cryptography: elliptic curves and cryptosystems.

	The balance between those parts and the details of the program may vary from year to year.
Inline resources	Moodle website https://moodle.uclouvain.be/
Bibliography	R. Crandall, C.B. Pomerance : Prime Numbers: A Computational Perspective, Springer, 2005. H. Davenport : The higher arithmetic. An introduction to the theory of numbers. 8th edition, Cambridge UP, 2008. K. Ireland, M. Rosen : A classical introduction to modern number theory, Springer, 2d edition, 1991. N. Koblitz: A Course in Number Theory and Cryptography, Springer, 2nd edition, 1994. J.P. Serre: Cours d'arithmétique, PUF, 1970.
Faculty or entity in charge	MATH

Programmes containing this learning unit (UE)

Program title	Acronym	Credits	Prerequisite	Learning outcomes
Additionnal module in Mathematics	APPMATH	5		🔍
Master [120] in Mathematics	MATH2M	5		🔍
Master [120] in Electrical Engineering	ELEC2M	5		🔍
Master [120] in Computer Science and Engineering	INFO2M	5		🔍
Master [120] in Mathematical Engineering	MAP2M	5		🔍
Master [120] in Data Science Engineering	DATE2M	5		🔍
Master [120] in Data Science: Information Technology	DATI2M	5		🔍